SEAN C. CUNNINGHAM, Bar No. 174931
sean.cunningham@dlapiper.com
KATHRYN RILEY GRASSO, Bar No. 211187
kathryn.riley@dlapiper.com
DAVID R. KNUDSON Bar No. 265461
david.knudson@dlapiper.com
DLA PIPER LLP (US)
401 B Street, Suite 1700
San Diego, CA 92101-4297
Telephone: 619.699.2700
Facsimile: 619.699.2701

TODD S. PATTERSON (*pro hac vice*)
todd.patterson@dlapiper.com
DLA PIPER LLP (US)
401 Congress Avenue
Suite 2500
Austin, Texas 78701-3799
Telephone: 512.457.7000
Facsimile: 512.457.7001

Attorneys for Defendant and Counterclaim Plaintiff SOPHOS INC. and Counterclaim Plaintiff SOPHOS LTD.

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

FORTINET, INC., a corporation,
Plaintiff,
v.

SOPHOS INC., a corporation, MICHAEL VALENTINE, an individual, and JASON CLARK, an individual,
Defendants.

SOPHOS INC. and SOPHOS LTD., corporations,
Counterclaim Plaintiffs,
v.

FORTINET, INC., a corporation,
Counterclaim Defendant.

CASE NO. 3:13-cv-05831-EMC

SOPHOS INC. AND SOPHOS LTD.'S OPPOSITION TO FORTINET'S MOTION FOR SANCTIONS

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page

CASES

TABLE OF AUTHORITIES
(continued)

Page

STATUTES

OTHER AUTHORITIES

I. INTRODUCTION

Fortinet's meritless motion for sanctions is designed to draw attention away from its failure to properly prosecute its equally meritless claim for trade secret misappropriation. Fortinet's chief complaint—that it did not get full access to the former Fortinet employees' computers and devices until recently—is a problem of Fortinet's own making. Under California statutory law, Fortinet was prohibited from commencing discovery related to its trade secret claims until it provided a proper disclosure of its alleged trade secrets. Fortinet failed to do so for more than 15 months, despite many demands by Sophos and a promise by Fortinet's lead counsel not to "back burner" the issue. Once Fortinet complied (marginally) with the statutory requirement in May 2015, Fortinet refused for six weeks to negotiate an acceptable protocol for the inspection of the computers and devices it was seeking. Among other things, Fortinet insisted that its outside counsel at Quinn Emanuel should have unfettered access to the former Fortinet employees' personal computers, which contain privileged and highly personal information. Minutes before the June 25 hearing, Fortinet finally relented and agreed to an acceptable review protocol, which is now underway.

Simply put, all of this—including this motion—could have been avoided if Fortinet had timely served its statutory disclosure of trade secrets when this case began (it did not) and immediately agreed to an acceptable review protocol for its former employees' personal computers (it did not). By delaying both for more than 15 months, Fortinet has needlessly and greatly increased the cost of this litigation. If anything, Fortinet should be sanctioned for its dilatory conduct. Having said that, sanctions are an extraordinary remedy reserved for vexatious conduct or acts of bad faith. Fortinet's dilatory conduct likely was motivated by its inability to articulate its alleged trade secrets. But certainly there is nothing Sophos did or failed to do that comes close to warranting sanctions. Because Sophos's conduct was justified under the law, Fortinet's motion should be denied.

/////

/////

/////

I. SANCTIONS ARE AN EXTRAORDINARY REMEDY THAT ARE NOT WARRANTED HERE.

Sanctions under 28 U.S.C. § 1927 are an "extraordinary remedy" and are limited to circumstances where an attorney multiplies the proceedings "unreasonably and vexatiously." 28 U.S.C. § 1927; *Torrisi v. Hunt & Henriques Law Firm*, No. SACV 10-1697-JST, 2012 WL 691450, at *3 (C.D. Cal. Mar. 1, 2012). An award of sanctions requires a finding that an attorney acted recklessly or in bad faith. *Lahiri v. Universal Music & Video Distrib. Corp.*, 606 F.3d 1216, 1219 (9th Cir. 2010). The bad faith requirement sets a "high threshold," and a court accordingly must exercise its power to sanction under Section 1927 with "extreme caution." *Torrisi*, 2012 WL 691450, at *3; *Oliver v. In-N-Out Burgers*, 945 F. Supp. 2d 1126, 1129 (S.D. Cal. 2013); *see also, e.g., Calgene, Inc. v. Enzo Biochem, Inc.*, No. CIVS-93-0195(EJG-GGH), 1993 WL 645999, at *3 (E.D. Cal. Aug. 27, 1993) (finding discovery conduct did not rise to sanctionable conduct, noting the court "will not turn the sanctions rules into a vehicle for punishment of every attorney transgression during discovery"); *Integrated Circuit Sys., Inc. v. Realtek Semiconductor Com., Ltd.*, No. C00-4035 MMC(BZ), 2002 WL 532122, at *1-2 (N.D. Cal. Apr. 5, 2002) (finding discovery disputes "certainly" did not constitute bad faith such to warrant sanctions under 28 U.S.C. § 1927).

Additionally, Rule 37 of the Federal Rules of Civil Procedure permits a court to impose sanctions against a party or the party's attorney for discovery violations. Fed. R. Civ. P. 37. Under Rule 37, the standard of sanctionable misconduct is generally one of objective reasonableness. *Marquis v. Chrysler Corp.*, 577 F.2d 624, 642 (9th Cir. 1978). Discovery conduct is "substantially justified if it is a response to a 'genuine dispute or if reasonable people could differ as to the appropriateness of the contested action.'" *MGA Entm't, Inc. v. Nat'l Products Ltd.*, No. CV 10-07083 JAK SSX, 2012 WL 4052023, at *2-3 (C.D. Cal. Sept. 14, 2012) (quoting *Devaney v. Continental American Ins. Co.*, 989 F.2d 1154, 1163 (11th Cir. 1993)). Accordingly, "the Ninth Circuit has declined to extend these sanctions to general discovery disputes under the rule." *Network Caching Tech., LLC v. Novell, Inc.*, No. C-01-2079 VRW, 2003 WL 21699799, at *3 (N.D. Cal. Mar. 21, 2003); cf. *Finander v. Los Angeles Unified Sch.*

Dist., 320 F. App'x 821 (9th Cir. 2009) (affirming grant of sanctions where party "flouted basic discovery obligations, violated court orders, deprived defendants of a meaningful opportunity to prepare for trial, and ignored multiple warnings regarding sanctions").

Courts also have inherent power to impose sanctions. Such inherent power, however, "is not a broad reservoir of power, ready at an imperial hand, but a limited source; an implied power squeezed from the need to make the court function." *Chambers v. NASCO, Inc*., 501 U.S. 32, 42 (1991); *see also Oliver v. In-N-Out Burgers*, 945 F. Supp. 2d 1126, 1129 (S.D. Cal. 2013) ("Because inherent powers are shielded from direct democratic controls, they must be exercised with restraint and discretion.") (quoting *Roadway Express, Inc. v. Piper*, 447 U.S. 752, 764, 100 S. Ct. 2455, 65 L. Ed. 2d 488 (1980)). To impose sanctions under the court's inherent power, a showing of bad faith is required. *Zambrano v. City of Tustin*, 885 F.2d 1473, 1478 (9th Cir. 1989). "[A]n inherent powers sanction is meant to do something very different than provide a substantive remedy to an aggrieved party. An inherent powers sanction is meant to 'vindicate judicial authority.'" *Mark Indus. v. Sea Captain's Choice*, 50 F.3d 730, 733 (9th Cir. 1995) (quoting *Chambers v. NASCO, Inc*., 501 U.S. 32, 55, 111 S. Ct. 2123, 115 L. Ed. 2d 27 (1991)).

II. THE COURT SHOULD DENY FORTINET'S MOTION FOR SANCTIONS.

Sophos's conduct with respect to Fortinet's trade secret discovery demands was proper, justified and necessary, given Fortinet's failure to prosecute its trade secret misappropriation claims. Contrary to Fortinet's accusations, Sophos did not engage in any reckless, intentionally deceitful, or bad faith conduct, let alone any conduct that would warrant sanctions.

A. Sanctions Under Section 1927 Are Unwarranted, Because Sophos's Refusal To Engage In Trade Secret Discovery Until May 2015 Was Justified Under The Law.

Sanctions are not warranted under 28 U.S.C. § 1927, because Sophos's counsel did not "unreasonably and vexatiously" multiply the proceedings. On the contrary, Sophos's conduct was justified at every turn under well-established law.

/////

/////

/////

1. Sophos First Requested That Fortinet Comply With Its Statutory Obligations Under California Code of Civil Procedure § 2019.210 In March 2014.

Contrary to Fortinet's false portrayal of Sophos as "delaying" discovery, it was Sophos who first asked Fortinet back in March 2014 to comply with its obligations under California Code of Civil Procedure § 2019.210. *See* Declaration of Sean C. Cunningham in Support of Sophos Inc. and Sophos Ltd.'s Opposition to Fortinet's Motion for Sanctions ("Cunningham Decl.") at ¶ 3. In fact, by Sophos's count, it asked Fortinet nearly 20 times over 14 months to serve a proper disclosure of its alleged trade secrets. Cunningham Decl. at ¶ 4.

The requirement of CCP § 2019.210 is simple and plain:

> In any action alleging the misappropriation of a trade secret under the Uniform Trade Secrets Act (Title 5 (commencing with Section 3426) of Part 1 of Division 4 of the Civil Code), before commencing discovery relating to the trade secret, the party alleging the misappropriation shall identify the trade secret with reasonable particularity subject to any orders that may be appropriate under Section 3426.5 of the Civil Code.

(Emphasis added.) The statute does not say a trade secret plaintiff "may" identify its trade secrets with reasonable particularly; it says "shall." Section 2019.210 has several well recognized purposes:

> First, it promotes well-investigated claims and dissuades the filing of meritless trade secret complaints. Second, it prevents plaintiffs from using the discovery process as a means to obtain the defendant's trade secrets. Third, the rule assists the court in framing the appropriate scope of discovery and in determining whether plaintiff's discovery requests fall within that scope. Fourth, it enables defendants to form complete and well-reasoned defenses, ensuring that they need not wait until the eve of trial to effectively defend against charges of trade secret misappropriation.

Perlan Therapeutics, Inc. v. Superior Court, 178 Cal. App. 4th 1333, 1343 (2009), *citing Advanced Modular Sputtering, Inc. v. Superior Court*, 132 Cal. App. 4th 826, 833-34 (2005). As the California Court of Appeal recently held: "It is critical to any [UTSA] cause of action—and any defense—that the information claimed to have been misappropriated be clearly identified. Accordingly, a California trade secrets plaintiff must, prior to commencing discovery, 'identify the trade secret with reasonable particularity.'" *Altavion, Inc. v. Konica Minolta Sys. Lab., Inc.*, 226 Cal. App. 4th 26, 43 (2014) (citing CCP § 2019.210).

Critically, Section 2019.210 prevents a trade secret plaintiff from "reverse-engineering" its alleged trade secrets by first obtaining materials in discovery, then claiming those materials to be its misappropriated trade secrets. *Brescia v. Angelin*, 172 Cal. App. 4th 133, 147 (2009) (Section 2019.210 permits defendant to "use that level of detail to determine the limits of the trade secret by investigating whether the information disclosed is within the public domain (meaning it is not a trade secret), or to develop the defenses of independent development or ready ascertainability (meaning there was no misappropriation)."). This "reverse-engineering" is precisely what Fortinet has been trying to do throughout this case, and continues to try to do with its inspections of its former employees' devices.

In May 2014, rather than complying with Section 2019.210, Fortinet served a broad, generic list of categories of alleged trade secrets in response to a Sophos interrogatory. Fortinet Ex. BB at 18-23.[1] In that initial response, Fortinet tried to claim as "trade secrets" generic things like information about its employees (including, unbelievably, their salaries, responsibilities, and skill sets). Fortinet also tried to claim as trade secrets its generic price lists and information about its business partners, all of which is easily obtainable on the Internet, including Fortinet's own website.

In multiple meet-and-confer calls and letters in May and June 2014, Sophos explained why this categorical listing did not come close to satisfying the statute. Sophos explained that California courts have held that broad, generic categories of purported trade secrets are insufficient under Section 2019.210, and Sophos made clear that "[i]t is particularly important to resolve this issue before any Sophos employees are deposed." Sophos Ex. 1 at p. 2. In response, Fortinet did nothing. In July 2014, Sophos again demanded a proper Section 2019.210 disclosure so the parties could commence trade secret-related discovery. Cunningham Decl. at ¶ 5(f). Again, Fortinet did nothing.

/////

[1] All references to lettered exhibits are to the exhibits attached to the Declaration of John M. Neukom in Support of Fortinet, Inc.'s Motion for Sanctions (Dkt. No. 179). All references to numbered exhibits are to the exhibits attached to the accompanying Cunningham Declaration.

On August 1, 2014, Sophos wrote to Fortinet to remind Fortinet that no trade secret-related discovery could commence until Fortinet complied with Section 2019.210. Sophos Ex. 2 at p. 1. Fortinet did not respond. On August 4, Sophos's counsel called Fortinet's counsel to say that Sophos was planning to move to compel a satisfactory Section 2019.210 disclosure from Fortinet, especially in light of the upcoming depositions of Sophos's employees. Cunningham Decl. at ¶ 5(h). The next day, Fortinet cut and pasted its initial interrogatory response into a document titled "Fortinet's Identification of Trade Secrets Pursuant to CCP § 2019.210." *Compare* Fortinet Ex. BB *with* Ex. CC. On August 13, the parties met and conferred, but Fortinet again refused to serve a proper Section 2019.210 disclosure, so Sophos sent Fortinet its portion of a joint discovery letter addressed to this Court and offered to continue the meet and confer process. Sophos Ex. 3. On August 27, the parties engaged in a final meet and confer that did not resolve the dispute. Cunningham Decl. at ¶ 5(m). On August 28, rather than providing its portion of the joint letter, Fortinet agreed to supplement its Section 2019.210 disclosure. Sophos Ex. 4.

On September 5, 2014, Fortinet served a supplemental Section 2019.210 disclosure, which again came nowhere close to satisfying the statute. Fortinet Ex. DD. On September 12, 2014, the parties discussed the deficiencies in Fortinet's supplemental disclosure, but did not resolve anything. Cunningham Decl. at ¶ 5(o). On that call, Fortinet's lead counsel promised that Fortinet would not "back burner" the issue of further supplementing its trade secrets disclosure. But nearly three weeks later, Fortinet had not responded, so Sophos's counsel sent an email to Fortinet's counsel, stating:

> We are still waiting on your response to our last comments about the trade secret disclosure. When we spoke on Friday, September 12, you said that you were not going to back burner the issue. I understand everyone is very busy, but we need to know by 5pm pacific tomorrow Fortinet's response.

Sophos Ex. 5. The next day, Fortinet's counsel responded: "We will certainly try to get back to you on this today. If not today, I expect by Monday." *Id.*

But Fortinet did not get back to Sophos that day, or the next Monday, or the next week, or the next month, or the month after that. In fact, Fortinet did not say a word about its trade secrets claims for the next four months, including during the November 2014 arbitration hearing before

Judge Komar. In that arbitration, Fortinet had pled contract-based trade secret misappropriation claims against its former employees Mike Valentine and Jason Clark. Fortinet Exs. A, B. But during the arbitration hearing, Fortinet did not ask a single question, make a single argument, or offer a single piece of evidence to support those claims. In their pre-hearing brief, Mr. Valentine and Mr. Clark pointed out that Fortinet's trade secrets claim was a red herring, in part because "Fortinet cannot even identify with reasonable particularity what its so-called 'trade secrets' are." Sophos Ex. 6. Fortinet did not respond, but instead abandoned its trade secrets claims against Mr. Valentine and Mr. Clark in the arbitration.

Not surprisingly, it was Sophos who restarted the discussions about Fortinet's deficient disclosure of alleged trade secrets in February 2015. In its February 23, 2015 responses to Fortinet's Third Set of Requests for Production of Documents, Sophos lodged objections to Fortinet's trade secret-related discovery requests on the grounds that Fortinet still had not complied with Section 2019.210. Fortinet Ex. F. Sophos made similar objections in response to Fortinet's Rule 30(b)(6) deposition notice on March 18 (Sophos Ex. 7) and in response to Fortinet's First Set of Requests for Inspection on April 8, 2015. Fortinet Ex. H. Presumably it was these objections that prompted Fortinet to finally serve its Second Supplemental Identification of Trade Secrets on May 1, 2015. Fortinet Ex. EE.

All told, it took 15 months and nearly 20 demands by Sophos for Fortinet to serve a disclosure of its alleged trade secrets that comes anywhere close to complying with Section 2019.210. If Sophos's intent was to try to delay trade secret-related discovery, it would not have hounded Fortinet to provide a proper Section 2019.210 disclosure. As it was, even though Fortinet had not complied with Section 2019.210, Sophos permitted Fortinet to extensively question the former Fortinet employees at their 2014 depositions on many trade secret-related topics. Cunningham Decl. at ¶ 6.

On May 11, 2015, Sophos agreed to accept Fortinet's latest Section 2019.210 disclosure so the parties could complete the remaining discovery, including the inspections of the former Fortinet employees' personal computers. Immediately thereafter, the parties began to discuss Fortinet's then-pending Requests for Inspection, which are at the core of Fortinet's accusations in

this motion. It is Fortinet's fault, not Sophos's, that the ensuing dispute about these inspections arose at the close of fact discovery. And the fact that Fortinet is just now getting documents it believes are "potentially relevant" is not a basis for sanctions. *See, e.g., Nuance Commc'ns, Inc. v. ABBYY Software House*, No. C 08-02912 JSW MEJ, 2012 WL 5904709, at *1 (N.D. Cal. Nov. 26, 2012) (denying request for sanctions and attorney's fees even where defendant provided no explanation for producing more than 10,000 pages of highly relevant documents after the close of discovery); *see also Creative Sci. Sys., Inc. v. Forex Capital Markets, LLC.*, No. 5:04-CV-3746-JF(RS), 2006 WL 305963, at *1 (N.D. Cal. Feb. 8, 2006) (denying request for sanction of attorneys' fees where party refused to produce relevant documents and respond to written discovery for more than four months).

2. Fortinet Refused To Negotiate An Appropriate Inspection Protocol For The Former Fortinet Employees' Devices, Which Further Delayed The Inspections.

Contrary to Fortinet's version of events, any delay in its inspection of the former Fortinet employees' devices after May 11 is on Fortinet, not Sophos. From May 11 through June 25, Fortinet steadfastly refused to agree to any inspection protocol that did not involve Fortinet's own lawyers at Quinn Emanuel having unfettered access to the data on the former Fortinet employees' personal computers. Sophos made it clear from the outset that it needed to be able to screen those devices for privileged documents and highly-sensitive personal information. Cunningham Decl. at ¶ 8; Fortinet Ex. GG at 1. Sophos's consistent position was (and is) that an outside expert should perform the inspections, with Fortinet's counsel having no access to the data until Sophos's counsel could screen it. Fortinet Ex. M at 4; Fortinet Ex. GG at 1.

On May 21, in a joint discovery letter regarding the inspections of Mr. Valentine's and Mr. Clark's computers, Sophos noted that it had already agreed to allow limited inspections of certain computers, but that "[a]ppropriate inspection procedures have not yet been worked out between the parties." Dkt. No. 130 at 7, n.4. On May 26 and 27, Sophos repeated its position that a protocol should be put in place for an outside expert to conduct the inspections. Fortinet Ex. M at 4; Fortinet Ex. GG at 1. Nonetheless, Fortinet's counsel demanded, at 9:55 pm on May 28, that its own lawyers be allowed to inspect the devices the following morning. Fortinet

Ex. GG at 2. Sophos again told Fortinet that its lawyers would not be allowed access to any device without a protocol in place to protect privileged documents and sensitive personal information on the devices. Fortinet Ex. GG at 1.

On June 2, after Fortinet insisted on filing yet another joint discovery letter with this Court, Sophos laid out its complete factual and legal bases for why any inspection must be done by an outside expert first, and not by Fortinet's own lawyers. Dkt. No. 138 at 6-7. This included examples of protocols that courts have ordered in similar situations. *Id*. On June 9, while still insisting that Sophos's protocol was "improper," Fortinet informed Sophos that it was working with an outside discovery vendor to conduct the inspections, and demanded that the devices be made available between June 10-12. Fortinet Ex. P at 4. Fortinet's counsel also acknowledged that the issue of its access to the devices would be decided at the then-scheduled June 25 hearing: "However, this issue [Fortinet's counsel's access to the computers] will be decided by the Court in Fortinet's most recent motion to compel and thus the parties need not debate it further." Fortinet Ex. P at 4.

On June 11, Sophos noted that "Fortinet still has not proposed a protocol, other than informing us it wants an outside vendor to inspect." Fortinet Ex. P at 2. Sophos again laid out its proposed inspection protocol:

> We have provided our position numerous times that, due to the inclusion of privileged and highly-sensitive information on these devices, that a qualified third party conduct the initial inspection, and identify which documents he/she believes needs to be produced. Sophos would then review those documents for privilege and responsiveness and then would produce them to Fortinet. Fortinet will not be allowed unfettered access to the entire contents of these machines."

Id., emphasis added. On June 12, Fortinet finally proposed "that its outside vendor inspect the devices, complying with Sophos' improper conditions." Fortinet Ex. P at 2. That very day, Sophos told Fortinet it would make the devices available to Fortinet's outside vendor on Tuesday, June 16, which it did. *Id*. at 1.

On June 25, just before the hearing with this Court, Fortinet finally relented and agreed to Sophos's inspection protocol. At the hearing, this Court ensured that Fortinet's outside lawyers

would not have direct access to anything on the computers before Sophos's counsel could screen the documents for privilege—just as Sophos had been suggesting all along:

> THE COURT: But I think the other concept that Mr. Cunningham is putting out there is, there doesn't appear to be any instance in which Fortinet will be able to access content on the mirror images or devices.
>
> MR. OLMOS: That will happen at Stroz Friedberg by those experts, yes.
>
> THE COURT: Okay. I'm sorry. But not – but just the expert is going to be looking. Okay.

6/25/15 Hrg. Tr. at 13:24-14:6.

Thus, by refusing for weeks to agree to a reasonable, commonly-used inspection protocol to protect the privileged information on the former Fortinet employees' computers, Fortinet itself caused a six-week delay in its inspection of these computers. Fortinet is now trying to make it Sophos's fault, but the Court should not permit Fortinet to rewrite history to cover for its own unreasonable behavior.

3. Sophos's Agreement To Allow Additional Inspections On The Day Of The June 25 Hearing Was A Reasonable And Appropriate Compromise.

Fortinet makes much about Sophos's agreement to permit additional inspections of devices in the attorney lounge before the hearing on Fortinet's motion to compel. Indeed, one of the bases for Fortinet's request for sanctions is "[r]efusing to concede Fortinet's two motions to compel even as late as the afternoon before the hearing in front of Judge Ryu." Mot. at 22.

First, Sophos was not required to "concede" any motion to compel, particularly when there were legitimate disputes that required the Court's intervention.[2] Fortinet's outside lawyers insisted on having unfettered access to the former Fortinet employees' personal computers. Fortinet also was seeking access to many devices, such as personal computers and phones, that Fortinet ultimately conceded on the parties' July 10, 2015 meet and confer call that it had no

[2] Fortinet incorrectly claims that it "prevailed on its two motions to compel." Mot. at 4. On the contrary, this Court denied Fortinet's motions as moot because the parties reached a compromise on their own. Dkt No. 161.

evidence to suggest had ever been used for Fortinet business. Sophos was justified in seeking this Court's guidance with respect to these legitimate disputes. The fact that the parties resolved their disputes just before the hearing was commendable, not a basis to seek sanctions.

Second, Sophos's "change in positions" regarding the inspections of the various devices had nothing to do with multiplying the proceedings unreasonably or vexatiously. Mot. at 10-11. On the contrary, Sophos compromised with Fortinet on the devices to be inspected once Fortinet agreed to Sophos's inspection protocol. *See* Dkt. Nos. 161, 170. Sophos did so to reduce or eliminate the disputes for the Court's consideration and decision. Parties compromise all the time, and they should be encouraged to do so. Sophos's willingness to compromise with Fortinet is the opposite of sanctionable conduct.

4. The Search Results On The Former Fortinet Employees' Computers Do Not Demonstrate Misconduct.

Fortinet claims that early search results from its discovery vendor "already show how egregiously wrong it was for Sophos to have withheld these materials for so long." Mot. at 19. Setting aside for the moment that the delay in trade secret-related discovery falls squarely on Fortinet, the large number of hits on the search terms that Fortinet's discovery vendor is running on the computer images does not demonstrate anything of consequence. Although Fortinet has identified and requested production of several hundred thousand files (mostly emails) from its searches, that number is not surprising, for several reasons.

First, Fortinet already knew that its former employees retained Fortinet data on their personal computers. Multiple former Fortinet employees, including Mike Valentine, testified at depositions taken in Fall 2014 that (1) Fortinet permitted them to use their personal computers for work business, including email, (2) they were not asked to return those materials or delete them when they left the company, and (3) they still had the Fortinet data on their personal computers at the time of their depositions. In particular, Fortinet's lead counsel elicited the following testimony in early October 2014 about Mr. Valentine's use of his personal Apple laptop for Fortinet business:

/////

> Q. Prior to leaving Fortinet, did you ever engage in any work e-mail or any work business while using your Apple laptop?
>
> A. Prior to Fortinet?
>
> Q. Prior to leaving Fortinet.
>
> A. Yes. I used that -- I would – in combination. It was the small one, I would typically use it on the road and then use the big one in the office. Yes.
>
> Q. Okay. And you could send e-mails on your Fortinet address through that Apple laptop, correct?
>
> A. Correct, yes.
>
> Q. And you still have that Apple laptop today?
>
> A. I do.
>
> Q. Have you deleted any files from that Apple laptop?
>
> A. I have not.

Sophos Ex. 8, October 6, 2014 Valentine Depo. at 266:23-267:14. Former Fortinet employee Kendra Krause also testified in October 2014 that she primarily used her personal Apple computer for work at Fortinet, and that Fortinet's IT department helped set it up, even transferring all of her Fortinet files to her personal computer. Sophos Ex. 9, October 2, 2014 Krause Depo. at 34:13-35:8; 254:11-258:4. When Ms. Krause left Fortinet, she asked what she should do with all of the documents and on her personal computer, and was told to talk to her boss and email him anything he might need. *Id.* at 35:11-24; 49:12- 50:22. She was never told to return anything, and she was never told to delete anything. *Id.* at 49:25-50:14. In fact, Ms. Krause testified that she did not delete anything from her personal computer, and currently has everything that she had while at Fortinet. *Id.* at 35:25-36:6. Ms. Krause then gave a detailed description of the types of documents that are still on her laptop, and when asked about the volume, replied "There's a lot of documents." *Id.* at 42:3-52:9.[3]

[3] These facts alone demonstrate that Fortinet's misappropriation of trade secrets claim has no merit. Fortinet cannot prove that it took reasonable measures to protect the secrecy of its data when employees were permitted—even encouraged—to use their own personal devices to conduct Fortinet business.

That these former employees retained Fortinet data from their employment—including all or a good portion of their Fortinet emails—was and is a surprise to no one, especially the Fortinet lawyers who took those depositions. What is "egregiously wrong" is that Fortinet waited for eight months after taking these depositions to serve a Section 2019.210 disclosure that was marginally acceptable in describing Fortinet's alleged trade secrets with "reasonable particularity." CCP § 2019.210.

Second, Fortinet is running extremely broad search terms, like "Fortinet" and "FTNT" (Fortinet's stock symbol) through its former employees' data, so it is not surprising that the search results are voluminous. The word "Fortinet" appears in every email sent, received, archived, or deleted from any Fortinet email account, so that term hits on all of the emails the former Fortinet employees retained on their personal computers. *See* Sophos Exhibit 13, Declaration of Paul T. French, at ¶ 9. In fact, Sophos's discovery vendor has confirmed that a single email to or from a Fortinet email address often returns multiple hits on the term "Fortinet." *Id.* at ¶¶ 8, 9. Fortinet also searched for the combination of "Fortinet" and "confidential," which is guaranteed to produce a large number of results, because the word "confidential" appears in the footer of virtually every Fortinet email. *Id.* at ¶ 9. Fortinet also searched for the term "Salesforce," which is a database Fortinet uses to store various customer and sales information. Fortinet has asked Sophos to produce every document containing that term. But the problem is that Sophos also uses a Salesforce database in its business, so all of the Sophos computers that Fortinet searched contain many, many references to Sophos's "Salesforce" database, virtually all of which are irrelevant.

Third, Fortinet apparently ran its search terms across all of the computer images its discovery vendor collected, which included two sets of image data from the same computers and smartphones taken at different times. Thus, the search results are exaggerated because they are returning thousands of duplicate hits on two images of the same computer or smartphone. *Id.* at ¶¶ 8, 9.

Fourth, as Fortinet knows, many of the search results are not human-created or human-readable files, such as cached web pages and web history files, system files, executable files,

graphics files (including .jpg and .png files), and even MP3 music files. *See Id.* at ¶ 3. Fortinet has included all of these file types in its "hit" count to inflate the total number of search results it claims to have identified.

In sum, Fortinet's claim that a high number of search results were identified on its former employees' computers and devices does not demonstrate any misconduct on the part of Sophos or its counsel. Simply because a document contains the words "Fortinet" or "confidential" does not make that document relevant, and it certainly says nothing about whether it falls within one of Fortinet's enumerated alleged trade secrets. As with everything else in its motion, Fortinet's accusations in this regard are designed to cover for Fortinet's failure to properly prosecute its trade secrets claim.

5. Sophos's Counsel Did Not Make Any "Knowingly False Or Intentionally Deceiving" Statements.

Fortinet levels unwarranted and unprofessional accusations at Sophos's counsel, accusing counsel of "knowingly false or intentionally deceiving" statements. Mot. at 2, 4, 21. Sophos's counsel take their obligations to the Court and to opposing counsel very seriously, and they confirm that no such false or deceiving statements were made. Cunningham Decl. at ¶ 25. Sophos addresses Fortinet's specific allegations below.

a. Sophos's Objections Based On Lack of Possession, Custody or Control Were Warranted In Light Of Fortinet's Overbroad Requests.

Fortinet first claims that Sophos's objections to Fortinet's Requests for Inspection based on lack of possession, custody or control amount to "knowingly" false statements. Mot. at 2. On the contrary, Sophos's objections were warranted because Fortinet's inspection requests encompassed many devices that are outside of Sophos's possession, custody or control, such as devices used by the former Fortinet employees that are no longer in those employees' possession. *See, e.g.*, Fortinet Ex. H at 1. Fortinet knows that many devices responsive to its inspection requests are no longer in the possession of the employees who had them while at Fortinet, including portable electronic storage devices. Fortinet also ignores that Sophos qualified its objections with the following statement:

> To the extent any such computer or device is within Sophos's possession, custody or control, Sophos will not permit the requested inspection unless and until Fortinet fully complies with its disclosure obligations required by CCP § 2019.210. Sophos is willing to participate in a final meet and confer regarding Fortinet's insufficient disclosures under CCP § 2019.210.

Ex. H at 2-3. It was only after Sophos served these objections that Fortinet served its Second Supplemental Identification of Trade Secrets Pursuant to Cal. Civ. Proc. Code § 2019.210. Sophos's objections were not knowingly false or intentionally deceitful; rather, they were clear and well justified.

Fortinet's statement that Sophos had imaged the devices in 2014 as "proof" of a knowingly false statement also lacks merit. During the parties' discussions regarding the inspections, Sophos's counsel repeatedly told Fortinet that Sophos's counsel had imaged the Sophos-issued laptops, but only had a few of the employees' personal computers, not every device Fortinet was demanding. Cunningham Decl. at ¶ 9. Sophos's objections to Fortinet's inspection requests based on lack of possession, custody or control were appropriate, particularly given that Fortinet knew several of the devices it had requested had been given away (three computers) or lost (one smartphone and numerous USB devices).

Fortinet also cites to the June 16, 2015 30(b)(6) deposition testimony of Jason Clark for its "proof" that Sophos had possession, custody and control of all of the devices Fortinet had requested. Mot. at 21. But Fortinet ignores that the questions related to what devices were collected and imaged by Sophos's counsel were beyond the scope of what Mr. Clark was designated to testify about, and Fortinet ignores Sophos's objections to those questions. *See, e.g.*, Fortinet Ex. V at 26:22-27:1, 27:7-17, 28:21-29:5, 130:23-131:6, 160:1-12; Fortinet Ex. V at Ex. 1. It simply is not true that Sophos's counsel had imaged "all of the devices Fortinet requested more than a year earlier," as Fortinet claims. Mot. at 21; Cunningham Decl. at ¶ 9.

b. Sophos's Statement That Scanning The Devices Would Be Burdensome Was And Is True.

Sophos's statement that scanning all of the devices would be unduly burdensome was and is true, because Sophos (1) had not scanned all of the devices previously, and (2) did not have all

of the requested devices in its possession at that time. And Fortinet ignores that it had demanded new scans of all of the devices. Fortinet Ex. T at 1; *see also* Dkt. No. 170 at 2. The burdensome nature of this request has proved true in the recent weeks, as all of the former Fortinet employees had to either personally deliver or courier their Sophos-issued laptops and their personal computers and smartphones to Fortinet's discovery vendor for imaging. It has been extremely burdensome on these individuals to have to give up their work computers (yet again) for an extended period of time. And despite being assured that these devices would be promptly returned, they were not. For example, Dolph Smith sent his devices to Fortinet's discovery vendor on Monday, June 29, 2015 by overnight delivery. Ryan Archer sent his devices on Tuesday of that week by overnight delivery as well. Fortinet had previously told Sophos's counsel that a standard laptop should only take 4-5 hours to image, and thus these computers and phones should have been returned no later than the day after Stroz received them. Sophos Ex. 10. But Sophos's counsel had to contact Fortinet the following Monday, July 6, to find out where Mr. Smith's and Mr. Archer's computers and devices were. With no explanation, Fortinet responded that "Both Smith and Archer were contacted today and Stroz is sending their devices back tonight via Fedex." Sophos Ex. 11. This was of no help to Mr. Archer, who was expecting to have his laptop back in plenty of time for a trip he was taking that night.

Sophos's assertion that the imaging (and re-imaging) of all of the devices Fortinet was requesting was unduly burdensome was and is true. That statement was the opposite of a knowingly false or intentionally deceitful statement.

c. Fortinet's Claim That Sophos's Counsel "Suggested" That They Only Had Personal Devices For Krause and Acosta Is False.

Contrary to Fortinet's statement (Mot. at 21), Sophos's counsel never "suggested" that the only personal devices they had were Ms. Krause's and Mr. Acosta's. At that point in time, the parties were disputing whether the personal devices of Mr. Valentine and Mr. Clark would be inspected. Sophos's counsel informed Fortinet that, excluding the Mr. Valentine and Mr. Clark's computers, it had available the images of the personal computers of Ms. Krause and Mr. Acosta. Ex. M at 4-5. The only other personal computer Sophos had imaged (besides Valentine's and

Clark's) was Dolph Smith's. The fact that Sophos's counsel did not mention Mr. Smith's computer was an inadvertent oversight, not an intentional misstatement. In fact, Fortinet ignores that just two weeks later, Sophos's counsel corrected the oversight when it notified Fortinet that it now also had just collected Rob Gattis' personal computer. Fortinet Ex. U at 4. The fact that Sophos's counsel omitted Mr. Smith's computer from an email, then corrected the oversight, obviously does not warrant sanctions.

d. Sophos's Alleged Assertion That It Had Already Produced All Relevant Evidence Did Not Include The Former Fortinet Employees Personal Devices Or Documents That Had Not Yet Been Reviewed

The footnote Fortinet cites (Mot. at 11) was intended to refer to documents in Sophos's possession that Sophos's counsel had previously identified and withheld from production as being potentially responsive to Fortinet's trade secret-related document requests. Once Fortinet produced its marginally adequate trade secrets disclosure, those documents were produced. That footnote, however, was not intended to and did not refer to the data on the former Fortinet employees' personal computers, which were subject to Fortinet's requests for inspection. It also did not refer to documents that Sophos's counsel had not yet reviewed, as the fact discovery period was still open.

6. Sophos's *Res Judicata* Argument Was And Is A Correct Statement Of The Law, Which Sophos Will Pursue At The Appropriate Time.

Fortinet also takes issue with the fact that Sophos asserted that *res judicata* bars Fortinet from taking a second bite at the apple in trying to prove its abandoned trade secrets claims against Mr. Valentine and Mr. Clark. Mot. at 22. Sophos's *res judicata* argument was and is a correct statement of the law, and Sophos fully intends to pursue that argument at the appropriate time. Contrary to Fortinet's counsel's assertion, Sophos did not agree to allow the inspection of Mr. Valentine's and Mr. Clark's computers because it had "reconsidered its res judicata objection." Neukom Decl. at ¶ 21. On the contrary, Sophos stated that it would allow these inspections to "avoid burdening this Court with at least one discovery dispute," and told Fortinet that "[b]y producing these documents and agreeing to a limited inspection, Sophos does not waive its right

to seek preclusion of these documents or related information under the doctrine of res judicata, nor does it concede that any document produced is a Fortinet trade secret (in fact, they are not)." Fortinet Ex. N. Given Sophos's explicit statement reserving its rights, Fortinet's counsel's statement is obviously wrong.

7. Sophos Did Not "Force" Fortinet To Take Its Own Noticed Rule 30(b)(6) Deposition.

Fortinet strangely claims that Sophos somehow "forced" Fortinet to take its own noticed 30(b)(6) deposition on trade secret misappropriation. Mot. at 22. Again, Fortinet omits critical facts.

First, as Sophos repeatedly told Fortinet, Fortinet's 30(b)(6) notice was directed to Sophos the company, and Mr. Clark was Sophos's Rule 30(b)(6) designee on those topics. Fortinet Ex. U at 2, 4. Sophos's testimony as to what it knew about any alleged trade secret misappropriation did not hinge on any inspections Fortinet would undertake, nor would the testimony have changed depending on the documents Fortinet might have shown Mr. Clark that day. As discussed above, it is a surprise to no one, particularly Fortinet's counsel, that the former Fortinet employees still have Fortinet documents in their possession, because Fortinet allowed these employees to retain documents when they left the company.

Second, June 16, 2015 was the day fact discovery closed. The hearing in front of this Court to sort out which inspections would be allowed, and under what conditions, was not scheduled to occur until June 25, nine days after the close of fact discovery. As Sophos told Fortinet, Sophos was not willing to extend this deposition beyond the close of fact discovery, particularly in light of the uncertainty of what would happen at the June 25 hearing. Fortinet Ex. U at 2, 4-5. Thus, Fortinet was free to take, or not take, the 30(b)(6) deposition of Sophos on June 16, as it saw fit. Fortinet could have declined to take the deposition, but it decided to go forward. This is simply not a case of Sophos multiplying the proceedings "unreasonably and vexatiously." It is a case of Sophos providing a witness to testify on topics that Fortinet noticed, on the last day of fact discovery.

/////

Taken individually or taken together, none of these baseless accusations warrant the "extraordinary remedy" of sanctions under 28 U.S.C. § 1927.

B. Sanctions Under Rule 37 Are Unwarranted, Because Sophos Complied With The Court's Orders.

Fortinet's only basis for seeking sanctions under Federal Rule of Civil Procedure 37 is its claim that Sophos violated the Court's June 30, 2015 (Corrected) Order (Dkt. No.170), which memorialized the agreements the parties reached on June 25. For several reasons, Fortinet's request for sanctions under Rule 37 is baseless.

First, Sophos provided its Accounting of Devices to Fortinet on June 29, as agreed. Fortinet Ex. Y. This Accounting listed the responsive devices currently in the possession of the former Fortinet employees, as well as devices that were previously unavailable or were no longer available, with an explanation as to why those devices were unavailable. For several employees, Sophos listed a "personal computer" as being unavailable for the simple reason that those employees do not own a personal computer. The Accounting also listed two computers that had been imaged within the last six months, which were therefore exempt from additional imaging. The Accounting also listed devices that had been wiped or reformatted and then given away.

Fortinet's chief complaint appears to be that Sophos did not identify any USB drives in this Accounting, despite Fortinet having provided Sophos with a list of USB devices that its discovery vendor claims had been connected to certain of the computers at some point in the past.[4] Mot. at 24; *see also* Fortinet Ex. T at 1. Sophos could not provide a list of USB devices in its Accounting because none of the former Fortinet employees have been able to locate any USB devices that may have been connected to their computers. Cunningham Decl. at ¶ 10. Also, several of the former Fortinet employees did not recognize the USB devices as they were identified by Fortinet. *Id*.

Sophos's Accounting of Devices contained a clear explanation as to why no USB devices were listed. Sophos told Fortinet: "To the extent any USB or other external drive devices are

[4] Fortinet acknowledges in its motion that these USB devices were purportedly connected to those computers "months and years" ago. Mot. at 18.

responsive to Fortinet's Requests, the former Fortinet employees are continuing to search for such devices, and will identify and produce them, if any exist and can be located." Fortinet Ex. Y at 1. This was all that was required under the Court's Corrected Order. See Dkt. No. 170 ("Fortinet will attempt to identify by manufacturer or name all USB devices it asserts were connected to the Former Fortinet Employees' personal laptops. Sophos will locate any such USB device that is still in the Former Fortinet Employees' possession and will provide images of those devices if located."). Sophos has done all it can to identify or locate these USB devices.

Fortinet specifically complains about the USB devices Ryan Archer testified about in his September 2014 deposition. Mot. at 18. Fortinet fails to inform the Court that Mr. Archer also testified that he routinely loses his USB devices and recently had to purchase another one because he could not find any of them. Sophos Ex. 12, September 23, 2014 Archer Depo. at 60:10-61:12.

Fortinet also complains about an "external hard drive" allegedly used by Dolph Smith to back up Fortinet data; however, there appears to be a misunderstanding as to what this "backup drive" is and what it was used for. Jason Clark, testifying as Sophos's 30(b0(6) designee on June 16, stated that he had spoken to Mr. Smith and confirmed Mr. Smith had backed up his Fortinet data. Fortinet Ex. V at 77:24-78:9. Mr. Clark referred to it as a "backup drive," which Fortinet's counsel pounced on as being an "external drive." Fortinet Ex. V at 78:10-18. Mr. Clark then stated it was a "data storage device." Fortinet Ex. V at 78:19-21. Following this testimony and following Fortinet's complaints about Sophos's Accounting of Devices, counsel for Sophos contacted Mr. Smith directly. Cunningham Decl. at ¶ 11. Mr. Smith has clarified that (1) he uses an external SSD drive that is connected to his personal Mac computer to make scheduled Time Capsule backups; (2) he has never used this drive to back up either his former Fortinet laptop or his current Sophos laptop; (3) the backup of his Fortinet data was done directly from his Fortinet laptop to his Sophos laptop via a home network, and that no external drive was used for the Fortinet backup. *Id.* So the Dolph Smith "external drive" Fortinet is seeking does exist, however, it was not ever used to back up that Fortinet data. Since Fortinet is already in possession of two separate forensic images of Mr. Smith's Sophos laptop, as well as two separate forensic images of his personal Mac computer, any separate image of this SSD drive would be redundant.

Fortinet's other complaint is that Sophos did not provide all the devices that Fortinet claims "were admittedly used to store Fortinet's data." Mot. at 24. Specifically, Fortinet complains that the three computers Sophos identified as having been wiped, reformatted and given away were not produced for inspection. But Fortinet omits that Sophos identified these three computers in its Accounting as being unavailable. Fortinet Ex. Y at 2-3. And although the parties did have a conversation about these computers on July 10, it was not a meaningful meet and confer, and certainly not one where Fortinet made any sort of good faith effort to resolve this dispute. At the beginning of the July 10 call, Fortinet's counsel announced a "proposal" where Sophos would stipulate to all of the relief Fortinet is seeking in its motion for sanctions or else Fortinet would file its motion. Specifically, Fortinet demanded that Sophos (1) pay Fortinet's attorneys' fees from May 1, 2015 onward, (2) pay the fees and costs of Fortinet's discovery vendor, (3) reimburse Fortinet for the June 16 deposition of Mr. Clark, and (4) agree to all of the non-monetary relief Fortinet now seeks. Fortinet gave no room for negotiation—the "deal" Fortinet proposed was agree to its terms "or else." Despite the hostile approach by Fortinet, Sophos attempted to understand the basis for Fortinet's motion, and sought to discuss the points Fortinet raised. When Sophos asked, for instance, how it could possibly produce Mr. DeHaven's old computer, which currently belongs to Mr. Clark's adult daughter, who is using it for college, Fortinet had no answer. Yet Fortinet still asserts that the failure of Sophos to produce this computer is a basis for sanctions against Sophos. Mot. at 24.

At the end of the day, Fortinet had no intention of trying to resolve anything. It wanted to file this motion, regardless what the actual facts were or are. Sophos even told Fortinet that it would consider Fortinet's position about the three wiped and transferred computers, but when Sophos did not provide an answer the following Monday, Fortinet filed its motion without talking to Sophos again.

In sum, Sophos fully complied with the parties' June 25 agreement and the Court's June 30 Corrected Order. Sophos's actions with respect to the three computers Fortinet complains of here were objectively reasonable, and if this failure to produce these three computers was a failure to comply with the Court's Order in any respect, it was "substantially

justified [as it was] a response to a 'genuine dispute or if reasonable people could differ as to the appropriateness of the contested action.'" *MGA Entm't, Inc. v. Nat'l Products Ltd.*, No. CV 10-07083 JAK SSX, 2012 WL 4052023, at *2-3 (C.D. Cal. Sept. 14, 2012). Thus, sanctions against Sophos under Rule 37 also are unwarranted.

III. CONCLUSION

Sophos acted reasonably and appropriately in response to Fortinet's own actions in this case. No individual accusation, nor any combination of accusations Fortinet has made against Sophos or its counsel, warrants sanctions of any kind. Fortinet's motion should be denied in its entirety.

Dated: July 31, 2015

DLA PIPER LLP (US)

By: */s/ Sean C. Cunningham*
SEAN C. CUNNINGHAM
KATHRYN RILEY GRASSO
DAVID R. KNUDSON
TODD S. PATTERSON

Attorneys for Defendant and Counterclaim Plaintiff SOPHOS INC. and Counterclaim Plaintiff SOPHOS LTD.

CERTIFICATE OF SERVICE

I, David R. Knudson, hereby certify that a true and correct copy of SOPHOS INC. AND SOPHOS LTD.'S OPPOSITION TO FORTINET, INC.'S MOTION FOR SANCTIONS has been served on all counsel of record via CM ECF on this 31st day of July, 2015.

/s/ David R. Knudson
David R. Knudson